METHOD AND SYSTEM FOR REMOTE MANAGEMENT OF PERSONAL SECURITY DEVICES

Field of Invention

The present invention relates to a data processing method for remote activation of personal security devices over a network for purposes of obtaining services or data from one or more remote computer systems. More particularly, the invention relates to a secure single-step method of activating and managing a personal security device through a communications pipe.

Background of Invention

The current art involving the management of personal security devices (PSD), for example, smart cards, requires a multi-step process where all the information necessary to use a personal security device is loaded into a PSD prior to distribution, including an initial personal identification number or PIN. The PSD is then sent to the end user followed by a separate letter containing the initial PIN which the user must enter the first time the PSD is used. Another current alternative, affixes an adhesive label containing a telephone number on a PSD prior to issuance. This label provides instructions for the end user to telephone a call center to activate the PSD before the device can be used.

The latter and former methods constitute multi-step processes, which adds considerably to the initial distribution and subsequent management costs of the PSDs. For example, in issuing smart cards, additional equipment, maintenance, labor and operating costs are required to generate either the separate mailings containing an initial PIN, or to generate adhesive labels to be placed on the smart cards and to operate the call centers which activate the cards.

Another major drawback of the current art concerns the lack of ability to manage information contained within the PSD after the device is issued. Currently, PSDs, which require changes, are either sent back to a central location or simply discarded and replaced with a new device. Both processes are time consuming and costly.

Summary of Invention

This invention provides a post issuance method of securely downloading and managing information inside the protected domain of a personal security device. This improvement over the current art utilizes a communications pipe as described in patent application OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device," which allows downloading of information into a blank personal security device and subsequently managing that information. For purposes of this invention, a blank PSD lacks proprietary algorithms and/or data but does contain an embedded runtime environment and optionally a unique identifier code.

In this invention, a communications pipe is established between a PSD via a client over a network to a remote computer system. This arrangement allows either the remote computer system maintaining the communications pipe or another remote computer system to download proprietary information such as authentication algorithms, cryptographic keys, credentials or certificates directly into a PSD connected to a local client through the communications pipe without disclosing proprietary information to the local client.

A major advantage of this method is it allows blank PSDs to be issued in bulk and activated at a future date without risk of compromise. Since no proprietary data is included in a bulk distribution, the PSDs are not usable to gain access to secure functions or data.

An example process by which a blank PSD becomes activated is as follows; an end user, who has previously received a blank PSD, connects the PSD to a local client and accesses a predetermined site over a network located on a remote computer system. The remote computer system may optionally perform end user authentication by some predetermined method such as prompting for a social security number, static PIN, mother's maiden name, etc. Alternatively, authentication may be implied using a unique identifier contained within the PSD.

Once the end user is properly authenticated or valid PSD connected, a remote computer system forms a communications pipe as described in co-pending patent application OCL-1, "Method and System for Establishing a Remote Connection to a Personal Security Device," and downloads, or causes another remote computer system to download, the necessary information through the communications pipe and into the PSD. The PSD may become activated upon completion of the process or as an additional security measure, the end user is prompted to devise and enter a unique PIN code to further protect access to the PSD.

In a second embodiment of this invention, a means to manage (e.g. upgrade, change, delete) PSD algorithms and data is facilitated by remotely gaining access to the devices and then downloading the changes directly into the PSDs, again without leaving proprietary information on the clients. Any changes necessary to proprietary information may be performed entirely within the secure domain of the PSD.

In both embodiments of the invention, all transactions occur within the secure domain of a PSD and a secure remote computer system, thus providing end-to-end security. When employed with the secure hub described in patent application OCL-2, "Method and System for Authentication Through a Communications Pipe," this improvement provides a centralized depository for tracking of PSD changes and greatly simplifies the management of large numbers of PSDs.

Brief Description of Drawings

FIG. 1A - is a general system block diagram for implementing present invention using a first remote computer system.

FIG. 1B - is a general system block diagram for implementing present invention using a subsequent remote computer system

FIG. 2 - is a detailed block diagram illustrating the direct transfer of proprietary information to a PSD.

FIG. 3 - is a detailed block diagram illustrating the remote transfer of proprietary information to a PSD.

Detailed Description of Preferred Embodiment

The need for secure network communications is paramount for sensitive business and government transactions. This invention provides an improvement over the current art by allowing issuance of generic personal security devices, which can be activated and customized at a later date.

The steps involved in activating a PSD and performing subsequent information management through a communications pipe are shown in FIG. 1 through 3. For purposes of demonstration, it should be assumed that any local authentications between the end user, client and local network domain have already been accomplished. In the preferred embodiment of the invention a secure communications protocol is employed over the network between the client and one or more remote computer systems. It is understood to one skilled in the art, that either embodiment of the invention will work with or without the use of secure communications protocols.

Referring now to FIG. 1A, a generalized system block diagram of the invention where Client 10 and a connected Personal Security Device 40 are connected over a network 45 with a remote computer system 50 using a communications pipe 75 as described in co-pending patent application OCL-1, "Method and System for Establishing a Remote Connection to a Personal Security Device." A remote computer system 50 maintains the communications pipe 75 and is available to transfer proprietary information "I" 165 through the communications pipe 75 and into the PSD 40.

In FIG. 1B, a second embodiment of the invention is depicted where a first remote computer system 50 acting as a secure hub as described in co-pending patent application OCL-2, "Method and System for Authentication Through a Communications

Pipe," provides a mechanism for a subsequent remote computer system 150 connected 85 to a network 45 to transfer proprietary information "I'" 165' into a PSD 40. In this embodiment of the invention, proprietary information 165' is received and processed by a first remote computer system 50. The proprietary information 165' is then sent by the first remote computer system 50, through the communications pipe 75 and into the PSD 40.

The network 45 may be a common network as in a virtual private networking arrangement or separate networks such as private intranet and public internet arrangements. No limitation is intended in the number of PSDs 40 and clients 10 forming communications pipes 75 with one or more remote computer systems 50, 150; nor should any limitation on the number of remote computer systems 50, 150 available for transferring proprietary information 165, 165' be construed from any of the depictions shown herein.

End user authentication is optional for activating blank PSDs or for deactivating PSDs already in use. In instances where access to a previously personalized PSD is desired, authentication transactions may be required as described in co-pending patent application OCL-2, "Method and System for Authentication Through a Communications Pipe," to facilitate secure access to the PSD. Once the authentication process has been accomplished, changes to proprietary information contained within the secure domain of the PSD are accomplished using the equivalent methodology described for blank card activation.

Proprietary information 165, 165' for injection into a PSD may originate on a remote computer system 50 supporting a communications pipe, other remote computer systems 150 or using any combination of remote computer systems.

Referring to FIG. 2, this drawing illustrates the transfer of proprietary information from a storage location over a network into a PSD using the remote computer system supporting the communications pipe. This drawing is applicable for either activating a blank PSD or changing information in an active PSD subsequent to authentication. In this embodiment of the invention, the proprietary information 165 is called from its storage location 160 within the remote computer system 50 or another remote computer system, which is local to, and communicating with, the remote computer system 50 maintaining the communications pipe 75.

After retrieval, the proprietary information 165 is sent 206 for processing into APDU format and encapsulation into the proper communications messaging format 204 as described in co-pending patent application OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device." After processing, the communications message 204 is sent through the network interface 130, into the communications pipe 75 over network 45 and received by the client 10 via a complementary network interface 130.

The incoming communications messages are sent 212 for processing where the APDU formatted information is separated as described in co-pending patent application OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device." The separated APDUs are then routed 216 through the hardware device port 5 and into 218 the PSD device interface 25. The incoming APDUs are then routed 30 into the secure domain 35 of the PSD 40 where the information is processed and stored by at least one embedded algorithm.

For newly issued PSDs lacking proprietary information, the embedded algorithm is installed by the PSD issuer and functions to manage the initial installation of proprietary information. For PSDs already containing proprietary information, the algorithm may be the same or a different algorithm, which may include cryptographic capabilities.

Referring to FIG. 3, this drawing illustrates the transfer of proprietary information from a remote storage location 160' over a network 45 and injection into a PSD 40 using a plurality of remote computer systems 50, 150. This embodiment of the invention involves retrieving proprietary information 165' from one or more 150 remote computer systems, sending 85 the proprietary information over a network 45 where the proprietary information is received and processed by a first remote computer system 50 which is supporting a communications pipe 75 and injected into the secure domain 35 of the PSD 40.

This embodiment of the invention is applicable for either activating a blank PSD or changing information in an active PSD subsequent to authentication. In instances where authentication is required, the remote computer system supporting the communications pipe may operate as a secure hub as described in co-pending patent application OCL-2, "Method and System for Authentication Through a Communications Pipe."

In this embodiment of the invention, the proprietary information 160' is called from a storage location inside a remote computer system 150 or another remote computer system, which is local to, and communicating with, the called remote computer system 150. The proprietary information "I" 165' is retrieved and sent 85 over the network 45 to the remote computer system 50 supporting the communications pipe 75 with the designated PSD 40.

Remote computer system 50 receives the proprietary information through the network interface 130 and routes the incoming proprietary information 165' for processing it 302 into APDU format and encapsulation into the proper communications messaging format 304 as described in co-pending patent application OCL-1, "Method and System for

Establishing a Remote Connection To a Personal Security Device." After processing, the communications message 304 is sent through the network interface 130, into the communications pipe 75 over network 45 and received by the client 10 via a complementary network interface 130.

The incoming communications messages are sent 312 for processing in 314 where the APDU formatted information is separated as described in co-pending patent application OCL-1, "Method and System for Establishing a Remote Connection To a Personal Security Device." The separated APDUs are then routed 316 through the hardware device port 5 and into 318 the PSD device interface 25. The incoming APDUs are then routed 30 into the secure domain 35 of the PSD 40 where the information is processed and stored by at least one embedded algorithm.

As previously described, for newly issued PSDs lacking proprietary information, the embedded algorithm is installed by the PSD issuer and functions to manage the initial installation of proprietary information. For PSDs already containing proprietary information, the algorithm may be the same or a different algorithm, which may include cryptographic capabilities.

The foregoing described embodiments of the invention are provided as illustrations and descriptions. They are not intended to limit the invention to precise form described. In particular, it is contemplated that functional implementation of the invention described herein may be implemented equivalently in hardware, software, firmware, and/or other available functional components or building blocks. Other variations and embodiments are possible in light of above teachings, and it is not intended that this Detailed Description limit the scope of invention, but rather by the Claims following herein.